Foreign National Cyber Access
Risk Assessment
Version 2.1
November 2, 2011

Division: PSC
Prepared by: K. Sidorowicz
Service/Computer/Cluster: Short Term Visitors

Number: FNCA-APS4
Date: April 2, 2014

Instructions:
1. Use the form below to assess the vulnerabilities of your environment. Please extend the form if your environment has features not discussed below.
2. Identify the access controls you have in place to manage the user's environment. In addition to the standard login authentication processes, consider default file permissions, WWW content access, ftp server access, file sharing, etc. Provide enough detail to explain your answer.
3. Answering Yes or No to a question does not disqualify a legitimate user from accessing a computer system. Rather these questions are designed to help you assess the risks involved in granting any user access to a computer system by highlighting potential concerns.
4. You should only need one of these vulnerability assessments for each computing environment. Please update this form if your environment changes significantly.
5. Keep this on file in your division.

If this user will be provided a computer:

	Vulnerabilities	Response/Access Controls
1.	Are there data or applications on the computer that this user will be using that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	No.
2	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data on his computer? For example	User does not have administrator access to system files. Configuration management ensures systems are installed and protected from non-authorized users.
2.1	Have you removed the inappropriate data or applications?	N/A
2.2	Are all users instructed in the secure management of data and applications?	Yes. All users take the ESH 223 computer protection training.
2.3	Does the computer system require authenticated access?	Yes
2.4	Can you uniquely identify users?	Yes.
2.5	Do you establish minimal default file permissions for all accounts?	Yes.
2.6	How do you verify file permissions are correctly set for data and applications?	Scans and Audits.

If this user will be provided network access to computer services (mail, ftp, etc.):

	Vulnerabilities	Response/Access Controls
3.	Are there data or applications on the servers that this user will access that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	No.
4.	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data stored on computers providing these services? For example:	Only System Administrators are allowed to login to the file servers. Account setup enables users to only access their share.
4.1	Does having access to this server enable unauthenticated access to a local intranet (by	No. These servers do not permit subsequest connection to other services.

	virtue of having an *division.anl.gov* address)?	
4.2	Does having an account on this server enable authenticated access to other computers?	N/A
4.3	Are other computers sharing file systems that may be accessible from this server (e.g. NFS, Windows file shares)?	N/A
4.3.1	If yes, how do you control network file access?	N/A
4.3.2	How do you verify network file permissions are correct?	N/A

If this user's network connection provides intimate[1] access to a computing environment:

	Vulnerabilities	Response/Access Controls
5.	Are there data or applications in the network vicinity of this user's computer that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	Since access to this computer lets the user behind the Laboratory firewall, the user could see all Laboratory services a regular employee could see. Thus the user could electronically "touch" numerous computers with sensitive data unless those computer owners have taken steps to isolate them.
6.	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data stored on computers in the vicinity? For example (consider using nmap on the subnet to identify open services):	Configuration management at the Laboratory ensures systems are installed and protected from non-authorized users.
6.1	Does having access to this computer enable unauthenticated access to a local intranet (by virtue of having an *division.anl.gov* address)?	Yes.
6.2	Does having an account on this computer enable authenticated access to other computers?	Yes. If requested by the Argonne host.
6.3	Are other computers sharing file systems that may be accessible to this computer (e.g. NFS, Windows file shares)?	Yes. But shares and filesystems are accessible only if authorized access is allowed.
6.3.1	If yes, how do you control network file access?	Configuration management ensures systems are installed and protected.
6.3.2	How do you verify network file permissions are correct?	Periodic scans and internal audits.

If this user has administrative privileges:

	Vulnerabilities	Response/Access Controls
7.	What is the scope of the administration privileges that this user has over the computer systems in your division? Example: Domain Administrator, E-Mail Administrator, Unix NIS, Desktop Administrator, etc	N/A
8.	Are there data or applications on the computer(s) that this user will be managing that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	N/A

---

[1] For example:What is visible in the Network? Are there unrestricted NFS exports on the local network? If a user runs tcpdump or places an ethernet interface in promiscuous mode, what will they see?

8.1	Do the data owners understand the confidentiality, integrity, and availability implications of this user's administrative privileges?	N/A
8.2	Have the data owners approved this user's access to administrative privileges?	N/A
10.	Does the user have remote access to the ANL network?	No.
10.1	Would remote access enable this user or an offsite accomplice to access sensitive data?	No. Only visitor access.
10.1.1	Have the data owners approved this user's remote access capabilities?	N/A.
11.	Do you have a process in place to minimize the permissions that this System Administrator must have to perform his/her work function?	N/A

Management approval:

12.	Has your division director accepted this risk assessment?	Yes.